REMARKS

Favorable reconsideration of this application is respectfully requested.

Claims 1-20 are pending in this application. Claims 18-19 were rejected under 35 U.S.C. § 101. Claims 1-20 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Application Publication 2004/0015689 to <u>Billhartz</u>.

Addressing first the rejection of claims 18 and 19 under 35 U.S.C. § 101, that rejection is traversed by the present response.

Claims 18 and 19 were rejected as directed to a program and not a computer-readable medium needed to realize a computer program's functionality. In response to that rejection each of claims 18 and 19 is amended by the present response to no longer be directed to a program, but to instead be directed to a "computer readable medium". The amendments to claims 18 and 19 are believed to address the rejection thereto under 35 U.S.C. § 101.

Addressing now the rejection of claims 1-20 under 35 U.S.C. § 102(e) as anticipated by <u>Billhartz</u>, that rejection is traversed by the present response.

Applicants respectfully submit the outstanding rejection is not fully considering the claim features relative to the disclosure in <u>Billhartz</u>. Independent claim 1 recites "a second identification information generator which generates second identification information including the service name, the inherent information and the encryption data", the encryption data including encrypted "first identification information including a service name of available service and inherent information". Independent claim 18 recites similar limitations. Thereby, in independent claims 1 and 18, and claims 2-6 dependent therefrom, the second information includes (1) a service name and inherent information and (2) data with the encrypted service name and inherent information.

Claims 7-17 and 19 recite determining whether a communication partner is trustworthy based on a result of comparing data obtained by decrypting encryption data

included in first identification information with the service name and the inherent information included in the first identification information.

In such ways claims 1-6 and 18 are directed to a transmission side and claims 7-17 and 19 are directed to a reception side. Claim 20 is directed to a configuration of both transmission and reception sides.

In the claims, a transmission side transmits encryption data obtained by encrypting a service name and inherent information, and additionally transmits the service name and the inherent information. A reception side can determine whether a result of decrypting the encryption data coincides with the also received service name and inherent information, and can thereby determine whether the transmission side is trustworthy. That is, according to operations that can be realized in the claimed invention, as a transmission side transmits encryption data obtained by encrypting a service name and inherent information, in addition to transmitting the service name and inherent information, the reception side can easily and accurately determine whether the transmission side is trustworthy.

If it is assumed that the transmission side transmits only the encryption data and the encryption data has been generated by using a secret key that the transmission side improperly acquired, the reception side may erroneously determine that the transmission side is trustworthy without noticing the improper acquisition of the secret key. Even when the transmission side transmits non-encrypted service name and inherent information, the reception side cannot determine whether the transmission side improperly acquires such information.

The claimed inventions can address such a situation since in the claimed inventions encryption data obtained by encrypting a service name and inherent information is transmitted in addition to transmitting the service name and the inherent information. Thereby, a reception side can confirm that the service name and inherent information are

correct and confirm that the correct service name and inherent information are included in the encryption data. Thus, the claimed inventions allow more accurately determining the credibility of a communication partner.

Applicants submit the claimed features clearly distinguish over Billhartz.

Billhartz is not directed to such operations as discussed above as Billhartz merely discloses a technique in which encryption data is transmitted using a public key and a private key between a first a node and a second node. Billhartz does not disclose nor suggest that encryption data is obtained by encrypting a service name and inherent information, and that such encryption data is transmitted in addition to transmitting the service name and the inherent information. As a result, Billhartz neither discloses nor suggests that encryption data included in reception information is decrypted, the service name and inherent information included in the reception information is compared with the decrypted information, and that it is thereby determined whether a communication partner is trustworthy.

With respect to the features discussed above of generating second information that includes the service name, the inherent information, and the encryption data, and the encryption data includes an encrypted service name and inherent information, the outstanding Office Action cites Billhartz at page 3, paragraph [0027].[1] Applicants traverse that basis for the rejection. More specifically, paragraph [0027] in Billhartz states:

> [0027]   By way of example, the first and second nodes 11, 12 may be laptop computers, personal data assistants (PDAs), or any other devices suitable for use in mobile ad-hoc networks, as will be appreciated by those of skill in the art. As such, the wireless communications devices 21, 23 may be wireless modems, cellular devices, etc., and the controllers 22, 24 may be microprocessors, for example.

The above-noted disclosure in Billhartz does not disclose or suggest any situation in which second identification information is generated that includes (1) a service name and

---

[1] Office Action of March 12, 2007, page 4, first paragraph.

inherent information, and (2) an encrypted service name and inherent information. The cited disclosure in <u>Billhartz</u> at paragraph [0027] merely indicates communication between different nodes.

Moreover, applicants note <u>Billhartz</u> does not even disclose or suggest any type of encryption of first identification information, which includes a service name and inherent information. With respect to that feature the outstanding Office Action cites <u>Billhartz</u> at page 3, paragraph [0028]. However, that disclosure in <u>Billhartz</u> merely notes a node authentification based upon public/private key encryption. That disclosure in <u>Billhartz</u> is not directed to encrypting first identification information that includes a service name of an available service and inherent information.
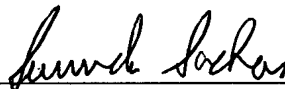
Similarly, the reliance on the disclosures in <u>Billhartz</u> at page 3 paragraphs [0031] and [0033] with respect to extracting a service name, inherent information, and encryption data, and decrypting such encryption data, is not at all directed to such claimed features. Those disclosures in <u>Billhartz</u> are merely directed to decryption via the public/private key. Those disclosures in <u>Billhartz</u> are not directed to the claimed features in which at a reception side a service name, inherent information, and encryption data is extracted, and the encryption data is decrypted to be compared with the received service name and inherent information.

In view of the foregoing comments, applicants respectfully submit claims 1-20 as written distinguish over <u>Billhartz</u>.

As no other issues are pending in this application, it is respectfully submitted that the

present application is now in condition for allowance, and it is hereby respectfully requested

that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK/SNS:law
I:\ATTY\SNS\24's\244986\244986US-AM.DOC

13